UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,783	12/10/2004	Satoshi Kitani	275870US6PCT	8620

22850 7590 09/19/2008
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
SU, SARAH	

ART UNIT	PAPER NUMBER
2131	

NOTIFICATION DATE	DELIVERY MODE
09/19/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	**Application No.** 10/517,783	**Applicant(s)** KITANI ET AL.	
	Examiner Sarah Su	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 June 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☒ Claim(s) *2,4,7,11,20 and 21* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 June 2008* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

FINAL ACTION

1. Amendment A, received on 26 June 2008, has been entered into record. In this amendment, claims 1-22 have been amended.

2. Claims 1-22 are presented for examination.

Response to Arguments

3. Applicant's arguments filed 26 June 2008 have been fully considered but they are not persuasive.

a. As to claim 1, it is argued by the applicant that Asano_1 and Oishi fail to teach acquiring a second seed or generating a second block key in the information processing apparatus instead of in an information-recording medium. The examiner respectfully disagrees. Oishi discloses acquiring a second seed (i.e. content key) by decrypting an encrypted second seed (0009, lines 8-11) and generating a second block key (i.e. storage encrypted content key) by encrypting (0009, lines 11-15). Furthermore, according to the amended preamble of claim 1, the information-processing apparatus comprises a plurality of encryption-processing units, and each unit includes encrypted data on an information-recording medium (lines 3-5). Therefore, according to this definition that defines the scope of the apparatus, because the medium is said to be included in the unit, then it is also included in the information-processing apparatus, and any process accomplished in the medium is also accomplished in the information-processing apparatus.

b. As to claim 9, it is argued by the applicant the same reasons as to claim 1. The examiner respectfully disagrees. Asano$_1$ discloses an information recorder (i.e. outside the information-recording medium) appending a time stamp (i.e. seed), which is formed as random data (i.e. generating) (0017, lines 5-9; 0018, lines 1-5) and storing it the seed in the leading area of the block data (i.e. on the medium) (0034, lines 5-6). Oishi discloses decrypting an encrypted content key to produce a content key at the data processing apparatus (i.e. outside the information-recording medium) (0014, lines 12-14) and also where the encrypted content key is decrypted at the storage device (i.e. stored on medium). Oishi also discloses that encryption/decryption of data is done at a data processing apparatus (i.e. outside the information-recording medium) (0009, lines 3-5, 8-11) and is transmitted from the storage device (0014, lines 3-5).

c. As to claims 14 and 22, the applicant makes the same argument as to claim 1. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the acquiring means and second generating means as part of the information-processing apparatus instead of the information-recording medium) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

d. As to claims 7, 8, 20 and 21, it is argued by the applicant that Asano2 does not teach "carrying out an authentication process…to generate a session key Ks." The examiner respectfully disagrees. Asano2 discloses that B received encrypted data from A and authenticates A (i.e. authentication process) and then B generates a session key (0449, lines 1-2, 10-11; 0450, lines 1-3).

Claim Objections

4. Claims 2, 4, 7, 11, 20, and 21 are objected to because of the following informalities:

a. In claim 2, line 18: "encrypted data" is unclear if it relates to "encrypted data" (claim 1, line 2);

b. In claim 4, line 2: "wherein said encryption-processing means also…" is unclear;

c. In claim 7, lines 8-9: "encrypted information" is unclear if it relates to "encrypted data" (claim 7, line 2);

d. In claim 7, line 11: "encrypted data" is unclear if it relates to "encrypted data" (claim 7, line 2);

e. In claim 11, line 3: "encrypted data" is unclear if it relates to "encrypted data" (claim 9, line 2);

f. In claim 20. line 7: "encrypted information" is unclear if it relates to "encrypted data" (claim 20, line 2);

g. In claim 20, lines 9 and 12: “encrypted data” is unclear if it relates to “encrypted data” (claim 20, line 2);

h. In claim 21, lines 10-11: “encrypted data” is unclear if it relates to “encrypted data” (claim 21, line 2).

Appropriate correction is required.

Drawings

5. The drawings were received on 26 June 2008. These drawings are acceptable.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claim 9 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 9 recites “generating, outside the information-recording medium, a first seed…” in lines 4-6 and “generating, outside the information-recording medium, a second seed…“ in lines 8-10. The specification discloses using these seeds to generate keys, but does not disclose generating the seeds outside the information-recording medium.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-4, 9-17, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asano et al. (EP 1185020 A1 and Asano$_1$ hereinafter) in view of Oishi et al. (EP 1039462 A2 and Oishi hereinafter).

As to claims 1, 14 and 22, Asano$_1$ discloses a system and method for information recording and reproducing, the system and method having:

> **first generating means for generating a first block key Kb1 on the basis of a first seed serving as key generation information set for the encryption-processing unit composing the encrypted data stored on the information-recording medium** [claims 1, 14, 22] (0031, lines 2-5);
>
> **decrypting means for decrypting the encrypted data stored on the information-recording medium based on the generated second block key Kb2** [claim 1, 14, 22] (0038, lines 2-4; 0052, lines 9-10);

Asano$_1$ does not expressly disclose:

acquiring means for acquiring a second seed by decrypting an encrypted second seed stored on said information-recording medium on the basis of the generated first block key Kb1 [claims 1, 14, 22];

second generating means for generating a second block key Kb2 by encrypting based on the acquired second seed [claims 1, 14, 22].

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by $Asano_1$, as evidenced by Oishi. Oishi discloses a system and method for encrypted data transfer, the system and method having:

acquiring means for acquiring a second seed (i.e. content key) **by decrypting an encrypted second seed stored on said information-recording medium on the basis of the generated first block key Kb1** [claims 1, 14, 22] (0009, lines 8-11) in order to allow for the content key to be changed without requiring re-encryption of the data;

second generating means for generating a second block key Kb2 (i.e. storage encrypted content key) **by encrypting based on the acquired second seed** (i.e. content key) [claims 1, 14, 22] (0009, lines 11-15) in order to allow for the content key to be changed without requiring re-encryption of the data.

Given the teaching of Oishi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the system and method of $Asano_1$ with the system and method of Oishi by using a decrypted seed to create a block key so that the data does not need to be re-encrypted if the content key is modified.

As to claims 2 and 15, Asano$_1$ discloses a system and method for information recording and reproducing, the system and method having:

master key generating means generates a master key on the basis of the master-key generation information [claim 2] (0011, lines 1-5);

recording key generating means generates first recording key K1 and second recording key K2 (i.e. device unique key) **on the basis of the generated master key** (i.e. LSI key) **and information read out from the information-recording medium** [claim 2] (0026, lines 3-7);

said first generating means generates said first block key Kb1 (i.e. device unique key) **by encrypting based on the generated first recording key K1 and the first seed** [claim 2] (0026, lines 8-10);

decoding means decodes encrypted data stored on the information-recording medium by decrypting based on the generated second block key Kb2 [claim 2] (0038, lines 2-4; 0052, lines 9-10).

generating a master key on the basis of master-key generation information read out from storage means [claim 15] (0011, lines 1-5);

generating two recording keys K1 and K2 (i.e. device unique key) **on the basis of the generated master key** (i.e. LSI key) **and information read out from the information-recording medium** [claim 15] (0026, lines 3-7);

generating said first block key Kb1 (i.e. device unique key) **by encrypting, based on the generated first recording key K1 and the first seed** [claim 15] (0026, lines 8-10);

decrypting the encrypted data stored on the information-recording medium by decrypting, based on the generated second block key Kb2 [claim 15] (0038, lines 2-4; 0052, lines 9-10).

Asano_1 does not expressly disclose:

said acquiring means acquires a said second seed by decrypting said encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1 [claims 2, 15].

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by Asano_1, as evidenced by Oishi. Oishi discloses a system and method for encrypted data transfer, the system and method having:

said acquiring means acquires a said second seed (i.e. content key) **by decrypting said encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1** [claims 2, 15] (0009, lines 8-11) in order to allow for the content key to be changed without requiring re-encryption of the data.

Given the teaching of Oishi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the system and method of Asano_1 with the system and method of Oishi by using a decrypted seed so that the data does not need to be re-encrypted if the content key is modified.

Asano$_1$ does not expressly disclose:

> **said second generating means generates a said second block key Kb2 by encrypting based on the acquired second seed and the generated second recording key K2** [claims 2, 15].

Asano$_1$ further discloses a system that **generates a block key by encrypting based on the acquired seed and the generated recording key** (i.e. device unique key) [claims 2, 15] (0026, lines 8-10), but does not expressly discloses that a second block key is generated based on a second seed and recording key.

Given the teaching of Asano$_1$, it would have been obvious to a person having ordinary skill in the art at the time the invention was made that generating a second block key using a second set of information is a mere duplication of parts. See MPEP 2144.04.

As to claims 3-4, 16-17, Asano$_1$ further discloses a system and method for information recording and reproducing, the system and method having:

> **unique key generating means generates a first title unique key and a second title unique key on the basis of the master key, a disc ID, which is information read out from the information-recording medium, and two title keys recorded on the information-recording medium** [claims 3, 4, 16, 17] (0020, lines 2-7);

said recording key generating means generates said first recording key K1 (i.e. result) **by encrypting based on the first title unique key and first information** (i.e. block seed) **read out from the information-recording medium** [claims 3, 4, 16, 17] (0024, lines 7-10).

Asano$_1$ does not expressly disclose:

generates said second recording key K2 by encrypting based on the second title unique key and second information read out from the information-recording medium [claims 3, 4, 16, 17].

Asano$_1$ further discloses a system that **generates a recording key by encrypting based on the title unique key and information read out from the information-recording medium** [claims 3, 4, 16-17] (0024, lines 7-10), but does not disclose that a second key is created based on a second set of information. Given the teaching of Asano$_1$, it would have been obvious to a person having ordinary skill in the art at the time the invention was made that generating a second recording key using a second set of information is a mere duplication of parts. See MPEP 2144.04.

As to claim 9, Asano$_1$ further discloses:

generating, outside the information-recording medium (i.e. in information recorder)**, a first seed** (i.e. ATS) **serving as key generation information set for each of encryption-processing units composing said encrypted data** (0017, lines 5-9; 0018, lines 1-5);

storing said first seed in the information-recording medium (0034, lines 5-6).

Asano$_1$ does not expressly disclose:

generating, outside the information-recording medium, a second seed service as key generation information encrypted on the basis of a first block key Kb1 generated on the basis of said first seed;

storing said second seed in the information-recording medium;

generating, outside the information-recording medium, an encrypted content encrypted on the basis of a second block key Kb2 generated on the basis of said second seed;

storing said encrypted content in the information-recording medium.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by Asano$_1$, as evidenced by Oishi.

Oishi discloses:

generating, outside the information-recording medium (i.e. at data processing apparatus)**, a second seed** (i.e. content key) **serving as key generation information encrypted on the basis of a first block key Kb1 generated on the basis of said first seed** (0014, lines 12-14) in order to allow for the content key to be changed without requiring re-encryption of the data**;**

storing said second seed in the information-recording medium (i.e. storage device) (0009, lines 8-10) in order to allow the seed to be provided;

generating, outside the information-recording medium, an encrypted content encrypted on the basis of a second block key Kb2 generated on the basis of said second seed (0009, lines 3-5, 8-11) in order to protect the content**;**

storing said encrypted content in the information-recording medium (0014, lines 3-5) in order to allow the encrypted content to be retrieved**.**

Given the teaching of Oishi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the system and method of Asano$_1$ with the system and method of Oishi by using a decrypted seed based on another seed so that the data does not need to be re-encrypted if the content key is modified and to protect the data and allow it to be retrieved.

As to claims 10-13, Asano$_1$ further discloses a system and method for information recording and reproducing, the system and method having:

where the first seed is stored inside control information set for each of encryption-processing units whereas the second seed is stored as encrypted information in a user-data area outside the control information [claim 10] (0022, lines 2-3; 0023, lines 3-6);

where the first seed (i.e. seed) **is stored in a user-data area as unencrypted data whereas the second seed** (i.e. data in block) **is stored in the user-data area as encrypted data** [claim 11] (0023, lines 3-6);

where the encrypted data is a transport stream packet (0018, lines 8-9), **the first seed is stored inside control information for a plurality of transport stream packets** (0018, lines 4-7; 0022, lines 2-3), **and the second seed is stored as encrypted information inside one of the transport stream packets in a user-data area outside the control information** [claim 12] (0023, lines 3-6);

where the first seed is stored inside a transport stream packet in a user-data area as unencrypted data whereas the second seed is stored as encrypted information inside the transport stream packet in the user-data area [claim 13] (0018, lines 4-10; 0023, lines 3-6).

10. Claims 5-6, 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asano$_1$ in view of Asano et al. (US 2002/0085722 A1 and Asano$_2$ hereinafter) and further in view of Oishi.

As to claims 5 and 18, Asano$_1$ discloses a system and method for information recording and reproducing, the system and method having:

generate a first block key Kb1 on the basis of a first seed serving as key generation information set for the encryption-processing unit [claims 5, 18] (0031, lines 2-5).

Asani$_1$ does not expressly disclose:

an authentication-processing unit configured to carry out an authentication process with the external apparatus to receive the encrypted

data read out from the information-recording medium in order to generate a session key Ks [claims 5, 18];

a plurality of encryption-processing units, each encryption-processing unit including said encrypted data stored on said information-recording medium [claim 5];

acquire a second seed by decrypting an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1 [claims 5, 18];

generate output-use encrypted information by encrypting data including the second seed on the basis of the session key Ks [claims 5, 18];

where the output-use encrypted information obtained as a result of the process to encrypt data including the second seed on the basis of the session key Ks is output through an interface [claims 5, 18].

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by Asano_1, as evidenced by Asano_2. Asano_2 discloses a system and method for protecting information by using secret information, the system and method having:

an authentication-processing unit configured to carry out an authentication process with the external apparatus to receive the encrypted data read out from the information-recording medium in order to generate a session key Ks [claims 5, 18] (0449, lines 10-11; 0450, lines 1-3) in order to authenticate processes between two systems;

a plurality of encryption-processing units (i.e. A,B), **each encryption-processing unit including said encrypted data stored on said information-recording medium** [claim 5] (0449, lines 1-2; 0451, lines 1-2) in order to process data separately;

generate output-use encrypted information (i.e. secret communication) **by encrypting data including the second seed on the basis of the session key Ks** [claims 5, 18] (0451, lines 7-9) in order to provide for authenticated communication between systems;

where the output-use encrypted information obtained as a result of the process to encrypt data including the second seed on the basis of the session key Ks is output through an interface (i.e. between A and B) [claim 5] (0451, lines 7-9) in order to provide for authenticated communication between systems.

Asano$_1$ in view of Asano$_2$ does not expressly disclose:

acquire a second seed by decrypting an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1 [claims 5, 18];

Nonetheless, this feature is well known in the art and would have been an obvious modification of the system and method disclosed by Asano$_1$ in view of Asano$_2$, as evidenced by Oishi.

Oishi discloses a system and method for encrypted data transfer, the system and method having:

acquiring a second seed (i.e. content key) **by decrypting an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1** [claims 5, 18] (0009, lines 8-11) in order to allow for the content key to be changed without requiring re-encryption of the data.

Given the teaching of Asano$_2$ in view of Oishi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the system and method of Asano$_1$ with the system and method of Asano$_2$ in view of Oishi by encrypting information based on a session key between authenticated systems in order to provide authentication communications and by using a decrypted seed so that the data does not need to be re-encrypted if the content key is modified.

As to claims 6 and 19, Asano$_1$ discloses a system and method for information recording and reproducing, the system and method having:

generate a master key on the basis of master-key generation information held by the information-recording medium drive [claims 6, 19] (0011, lines 1-5);

generate two recording keys K1 and K2 (i.e. device unique key) **on the basis of the master key** (i.e. LSI key) **and information read out from the information-recording medium** [claims 6, 19] (0026, lines 3-7);

generate the first block key Kb1 (i.e. device unique key) **by carrying out an encryption process based on the generated first recording key K1 and the first seed** [claims 6, 19] (0026, lines 8-10).

Asano$_1$ does not expressly disclose:

acquire the second seed by decrypting the encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1 [claims 6, 19];

generate the output-use encrypted information by encrypting data including the second seed and the second recording key K2 on the basis of the session key Ks [claims 6, 19];

output the output-use encrypted information including the second seed and the second recording key K2 through an interface [claims 6, 19].

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by Asano$_1$, as evidenced by Asano$_2$. Asano$_2$ discloses a system and method for protecting information by using secret information, the system and method having:

generate the output-use encrypted information by encrypting data including the second seed and the second recording key K2 on the basis of the session key Ks [claims 6, 19] (0451, lines 7-9) in order to provide for authenticated communication between systems;

output the output-use encrypted information including the second seed and the second recording key K2 through an interface [claims 6, 19]

(0451, lines 7-9) in order to provide for authenticated communication between systems.

Asano$_1$ in view of Asano$_2$ does not expressly disclose:

acquire the second seed by decrypting the encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1 [claims 6, 19].

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by Asano$_1$, as evidenced by Oishi. Oishi discloses a system and method for encrypted data transfer, the system and method having:

acquires a second seed (i.e. content key) **by decrypting the encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1** [claim 6] (0009, lines 8-11) in order to allow for the content key to be changed without requiring re-encryption of the data.

Given the teaching of Asano$_2$ in view of Oishi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the system and method of Asano$_1$ with the system and method of Asano$_2$ in view of Oishi by encrypting information based on a session key between authenticated systems in order to provide authentication communications and by using a decrypted seed so that the data does not need to be re-encrypted if the content key is modified.

11. Claims 7-8, 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asano$_2$ in view of Asano$_1$.

As to claims 7 and 20, Asano$_2$ discloses a system and method for protecting information by using secret information, the system and method having:

> **an authentication-processing unit for carrying out an authentication process with the external apparatus outputting the encrypted data in order to generate a session key Ks** [claim 7] (0449, lines 10-11; 0450, lines 1-3);
>
> **acquiring a seed** (i.e. content key) **used as key generation information and a recording key** (i.e. table key) **by decrypting, based on the session key, encrypted information received through the data input interface** [claims 7, 20] (0557, lines 9-15);
>
> **carrying out an authentication process with the external method outputting the encrypted data in order to generate a session key Ks** [claim 20] (0449, lines 10-11; 0450, lines 1-3);

Asano$_2$ does not expressly disclose:

> **generating a block key to be used as decryption key for decryption of encrypted data by encrypting, based on the seed and the recording key** [claims 7, 20];
>
> **decrypting, based on the block key, said encrypted data** [claims 7, 20].

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by Asano$_2$, as evidenced by Asano$_1$.

Asano$_1$ discloses a system and method for information recording and reproducing, the system and method having:

> **generating a block key to be used as decryption key for decryption of encrypted data by encrypting, based on the seed and the recording key** (i.e. device unique key) [claims 7, 20] (0026, lines 8-10) in order to recreate a key with which to restore original data;
>
> **decrypting, based on the block key, said encrypted data** [claims 7, 20] (0052, lines 9-10) in order to restore original data.

Given the teaching of Asano$_1$, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the system and method of Asano$_2$, with the system and method of Asano$_1$ by creating a block key from supplied data so that original data can be restored.

As to claims 8 and 21, Asano$_2$ discloses a system and method for protecting information by using secret information, the system and method having:

> **an authentication-processing unit for carrying out an authentication process with the external apparatus to receive the encrypted data read out from the information-recording medium in order to generate a session key Ks** [claims 8, 21] (0449, lines 10-11; 0450, lines 1-3);
>
> **a plurality of encryption-processing units, each encryption-processing unit including said encrypted data stored on said information-recording medium** [claim 8] (0449, lines 1-2; 0451, lines 1-2);

means for generating output-use encrypted information encrypting the decrypted data on the basis of the generated session key Ks [claims 8, 21] (0557, lines 5-7);

where the output-use encrypted information obtained as a result of encrypting of the decrypted data on the basis of the session key Ks is output through an interface [claims 8, 21] (0557, lines 5-11).

Asano$_2$ does not expressly disclose:

means for generating a block key on the basis of a seed serving as key generation information set for the encryption-processing unit [claims 8, 21];

means for acquiring decrypted data by decrypting the encrypted data stored on the information-recording medium on the basis of the generated block key [claims 8, 21].

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by Asano$_2$, as evidenced by Asano$_1$. Asano$_1$ discloses a system and method for information recording and reproducing, the system and method having:

means for generating a block key on the basis of a seed serving as key generation information set for the encryption-processing unit [claims 8, 21] (0031, lines 2-5) in order to recreate a key with which to restore original data;

means for acquiring decrypted data by decrypting the encrypted data stored on the information-recording medium on the basis of the generated

block key [claims 8, 21] (0052, lines 9-10) in order to restore original data with a key that was not directly transmitted with the data.

Given the teaching of Asano$_1$, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the system and method of Asano$_2$, with the system and method of Asano$_1$ by creating a block key from supplied data so that original data can be restored with a key that was not directly transmitted with the data.

Conclusion

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835.

The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2131

/Christopher A. Revak/
Primary Examiner, Art Unit 2131